Revista CIES – ISSN-e 2216-0167. Volumen 12. Número 2. Año 2021. Páginas 315-344. Dirección de Investigaciones – Institución Universitaria Escolme (Medellín, Colombia)

Tecnología en automatización robótica de procesos junto con las buenas prácticas de seguridad de la información

Sandra Juliet Gutiérrez Sierra
Administración de Sistemas Informáticos, Institución Universitaria Escolme, Medellín, Colombia, sjgutierrezs@escolme.edu.co

Christian Alejandro Agudelo Escobar
Administración de Sistemas Informáticos, Institución Universitaria Escolme, Medellín, Colombia, caagudeloe@escolme.edu.co

Recibido: 14/9/2021 - **Aceptado:** 5/10/2021 - **Publicado:** 21/10/2021

RESUMEN

Por medio de este artículo se pretende demostrar la importancia de adoptar procesos automáticos a través de la tecnología RPA en una organización, para mejorar los niveles de servicio y minimizar las operaciones manuales con el fin de llevar los sistemas de información de una manera más ágil y segura. Se contemplarán los conceptos relevantes, que van relacionados con el significado e importancia de un RPA, la automatización de procesos, los bots o agentes virtuales y las buenas prácticas de seguridad de la información. En el desarrollo del artículo se llevaron a cabo tres fases fundamentales en las cuales se contemplan como una primera fase, la identificación de procesos automatizados, la importancia del RPA en los procesos de las organizaciones frente a la necesidad de crear soluciones autónomas; en la segunda fase se realizó un análisis para brindar soluciones efectivas por medio de bots con el fin de automatizar las tareas repetitivas con el objetivo de aumentar la eficacia de los procesos en los sistemas de información; y finalmente en la tercera fase se hizó un análisis para las buenas prácticas de un RPA seguro, obteniendo soluciones basadas en la tecnología RPA que permitan a las organizaciones mejorar sus tiempos de respuesta, basados en el conjunto de las buenas prácticas de seguridad de la información. En conclusión, se estableció las pautas para lograr el buen funcionamiento de la tecnología RPA, y un análisis para el conocimiento del negocio de acuerdo con los temas tratados en el transcurso de este artículo.

Palabras clave: Bots; Automatización de procesos; seguridad informática.

ABSTRACT

Through this article it is intended to demonstrate the importance of adopting automatic processes through RPA technology in an organization, to improve service levels and minimize manual operations in order to carry out information systems in a more efficient way. agile and safe. Relevant concepts will be considered, which are related to the meaning and importance of an RPA, process automation, bots or virtual agents and good information security practices. In the development of the article, three fundamental phases will be

carried out in which are considered as a first phase, the identification of automated processes, the importance of RPA in the processes of organizations compared to the need to create autonomous solutions; In the second phase, an analysis will be carried out to provide effective solutions through bots in order to automate repetitive tasks in order to increase the efficiency of the processes in the information systems; and finally in the third phase an analysis will be made of the good practices of a secure RPA, obtaining solutions based on RPA technology that allow organizations to improve their response times, based on the set of good security practices of information . In conclusion, guidelines will be established to achieve the proper functioning of RPA technology, and an analysis for the knowledge of the business in accordance with the topics discussed in the course of this article.

Keywords: Bots; Process automation; IT security.

1. INTRODUCCIÓN

Con la tecnología RPA encontramos soluciones basadas en las buenas prácticas de seguridad de la información por medio de agentes virtuales o bots, que ayudan a mejorar la experiencia en relación con los usuarios, y a permitir ejecutar cada una de estas actividades de manera controlada con una participación de la fuerza laboral humana más mínima, aportando innovación, incorporando nuevas tecnologías a tareas manualmente irrealizables, reduciendo costos, aumentando la tasa de producción, y mejorando la calidad del servicio al cliente, la cual es importante medir mediante la utilización de modelos adecuados a cada sector (Mosquera-González et al., 2019).

Los BOTS son robots, los cuales tienen el mismo conjunto de habilidades que las personas, son una fuerza de trabajo digital que puede interactuar con cualquier sistema o aplicación. Por ejemplo, los bots pueden copiar y pegar, extraer datos web, hacer cálculos, abrir y mover archivos, analizar correos electrónicos, iniciar sesión en programas, conectarse a API y extraer datos no estructurados, además los bots se pueden adaptar a cualquier interfaz o flujo de trabajo, no es necesario cambiar los sistemas, las aplicaciones o los procesos empresariales existentes para realizar la automatización (Innovación y Tecnología, 2020), esta se puede implementar de acuerdo con lo que ya se viene trabajando en cada organización.

Los BOTS son importantes para la automatización de procesos con RPA y “desde 2018 hasta 2019, se estima que el gasto global en software de RPA ha aumentado de una manera significativa en un 57%, y a medida que avanza el tiempo con la pandemia, seguirá aumentando de una manera significativa, según investigaciones realizadas por la empresa Trycore (Vargas, s.f.). Lo que demuestra su popularidad a medida que la tecnología avanza.

También se puede ver que con la situación del COVID-19, esta tecnología ha explotado su potencial y ha contribuido de forma importante a luchar contra este virus, ya que por causa de la pandemia, se incrementó también el teletrabajo y a su vez el aumento de la carga laboral, por inconvenientes tal vez ajenos a los operadores, y uno de los causantes de estos problemas es la conexión a internet, que por su alto tráfico en la red obstaculiza el acceso a las aplicaciones de la empresa, y esto se ha logrado mejorar con los sistemas RPA que mediante los bots ayudan a realizar las tareas más repetitivas de la operación de manera

más ágil. De igual forma, estas herramientas de RPA permitieron mantener la continuidad de los procesos comerciales durante la pandemia (Siderska, 2021).

Por las anteriores razones, un gran número de empresas han adoptado esta tecnología como una vía rápida y fácil para automatizar tareas manuales. Demasiado beneficioso para la reducción de errores y aumento de la calidad en los procesos.

Otra solución que se puede lograr con gran eficiencia, y que ayuda a prevenir un riesgo, es el control de fraude en las organizaciones financieras. Facilita detectar movimientos extraños e inusuales, como, por ejemplo, en algunos tipos de cuentas bancarias; este software automatizado se ocupa de todas las operaciones de cuentas, trabajando de la mano, con la Inteligencia Artificial, lo cual es un primer paso hacia la adopción de esta tecnología que puede ir muy bien de la mano con los procesos RPA y de esta manera es posible investigar inmediatamente si se ha vulnerado la cuenta o no. Incluso, se ha indicado que las las organizaciones de servicios bancarios y financieros, seguros y atención médica han liderado la implementacióni de procesos de automatizacióin en el mundo (Anagnsote, 2018).

Se puede incluir también la gestión de la seguridad de la información, como otro factor importante que permite aumentar la eficacia de los procesos por medio de los bots, pues existen muchas posibilidades de que el error humano pueda desencadenar grandes consecuencias para la empresa al no contemplar la importancia de proteger la seguridad de la información y los datos de ella (Valencia-Arias et al., 2020).

La RPA no debe verse solo como una simple automatización, sino como un instrumento complejo que ofrece muchas ventajas con un enfoque en los beneficios para las partes interesadas internas y externas (Zelenka & Vokoun, 2021). Con la RPA se aumenta la precisión y control, mitigando los riesgos en la vulnerabilidad de los sistemas de información tanto a nivel de integridad o confidencialidad de los datos (Mayor-Ríos et al., 2019), generando garantía al cumplimiento de las normativas y al seguimiento de auditoría por medio de las tareas programadas, las cuales mejora notoriamente reducción de tiempos al equipo de trabajo, quienes pueden estar haciendo otras actividades igualmente críticas de la organización.

Por lo anterior, el presente trabajo tiene por objetivo identificar la importancia del RPA en los procesos de las organizaciones frente a la necesidad de crear soluciones autónomas.

2. MARCO TEÓRICO Y/O ANTECEDENTES

2.1. La Automatización Robótica de Procesos-RPA

De acuerdo con los avances tecnológicos, es importante hablar de la automatización robótica de procesos o RPA, que viene de la sigla en inglés (Robotic Process Automation). La RPA es un software que proporciona herramientas para crear sus propios robots digitales con el fin de emular automáticamente tareas operacionales que son rutinarias y repetitivas, interactuando con aplicaciones y fuentes de información de la misma manera

que lo harían los humanos, realizando actividades encomendadas y programadas por un sistema computacional.

A pesar de que hoy en día las empresas buscan la eficiencia en sus procesos al implementar esta tecnología, también debe tenerse en cuenta que no todas las tareas pueden ser resueltas mediante RPA, sin embargo, si puede ser la respuesta definitiva para tareas en donde no se necesita de conexión humana y que podrían considerarse estresantes.

2.1.1. ¿Para qué sirve el RPA?

Se adopta la tecnología RPA para que esas tareas repetitivas y de naturaleza sencilla sean ejecutadas en menor tiempo, este también aporta en la disminución de costos ya que un robot puede trabajar todos los días del año y en horario 24/7 sin tener que descansar, sin vacaciones, ni licencias, hay una disminución de la carga laboral, pudiendo así encaminar el talento humano en tareas más importantes, mejorando la eliminación de errores humanos y aumentando de esa forma calidad en los procesos. Adicional, las soluciones basadas en procesos automáticos se utilizan generalmente para actividades de gran volumen, repetitivas, basadas en reglas y con datos reales.

2.1.2. Aplicabilidad de los RPA

En el ámbito financiero aportan a su planificación y análisis mediante la utilización de datos históricos, también son utilizados para realizar consolidación de informes ejecutivos, captura de datos para reportes regulatorios, revisión de procesos para cuentas de clientes, pagos a proveedores, envío de e-mail informativo a clientes. También se aplica principalmente a las industrias relacionadas con los servicios financieros y bancos, seguros, manufactura, alta tecnología y comunicaciones, energía y servicios públicos. Los procesos que suelen automatizarse son la activación de tarjetas, reclamos de fraudes, preparación de nuevos negocios, creación de reportes automáticos, reconciliación de sistemas, generación de facturas, gestión de pedidos, informes de calidad, creación y configuración de cuentas entre muchos otros.

2.1.3. Beneficios de RPA

Con el desarrollo de robots con RPA se ofrece rentabilidad directa, por lo tanto, mejora la efectividad y producción de las organizaciones, poniendo soluciones a cualquier proceso y reduciendo los errores humanos, el tiempo y esfuerzo de los trabajadores a cero y libera recursos de los sistemas digitales y las horas de trabajo de las personas, mejora la producción y el servicio de los procesos creados al ser más eficientes.

Son preventivos operacionalmente y ayudan a la estrategia de crecimiento y transformación digital de la organización. Dentro de los beneficios que proporcionan los robots en el ámbito empresarial se encuentran los siguientes:

- Exactitud y precisión: los robots están programados para seguir las normas y cumplir su objetivo, no cometen errores en sus cálculos y son consistentes.

- Continuidad sin errores: todo lo que realizan estos RPA está monitorizado y en cualquier momento se puede modificar para que operen de acuerdo con nuevas regulaciones y estándares.

- Gran escalabilidad: los robots pueden realizar cantidad de operaciones en paralelo, desde entornos de escritorio de los sistemas digitales, hasta en sistemas en la nube.

- Disponibilidad: funcionan ininterrumpidamente las 24 horas del día, todos los días del año.

- Ahorro: las herramientas de RPA reducen hasta un 80% los costes de procesamiento.

2.1.4. Ventajas de los RPA

Algunas de las principales ventajas para adoptar este tipo de tecnología son, que para programar un bot no es necesario tener nociones de programación, así que cualquier persona que quiera aventurarse en este mundo del RPA lo puede hacer sin problemas, sin necesidad de tener habilidades de desarrollo y con un costo mínimo.

De acuerdo con investigaciones realizadas, se considera que otra de las ventajas más atractivas de automatizar la empresa, yace en la capacidad de lograr resultados acelerados con procesos uniformes que "respaldan la evolución de una cultura en la que los equipos de DevOps (Red Hat, s.f.a), según lo manifiesta Microsoft, al utilizar la tecnología Red Hat, ya que pueden concentrarse en compartir conocimientos, desarrollar habilidades y crear soluciones innovadoras, cubriendo la automatización de muchos procesos y ofreciendo ventajas competitivas para las organizaciones. De esta forma, se consigue la transformación digital de la organización y un avance en el camino hacia la futura aplicación de la Inteligencia Artificial en RPA.

2.1.5. Desventaja de los RPA

Se podría pensar que adoptar este tipo de tecnología se puede sentir como una amenaza laboral por desconocimiento por parte de algunas personas dentro de una organización, pero no lo es, el desplazamiento que genera solo afectaría en un futuro a las personas que ejecuten labores menos calificadas que sean repetitivas en su día a día, pero en general solamente es posible automatizar a través del RPA procesos repetitivos y poco complejos. A medida que la tecnología avance, los robots seguramente asumirán otras tareas más complejas que hoy en día todavía solamente pueden realizarse por los seres humanos.

Otra desventaja es que donde se tenía la necesidad de la antigua interacción humana esta se eliminaría por completo debido a encaminar este proceso dentro de una respuesta automática.

2.2. La automatización

Existe la tendencia a una sociedad automatizada, razón por la cual se hace necesario definir el concepto de automatización, como el uso de sistemas de software para crear

instrucciones y procesos repetibles para reemplazar o reducir la interacción humana en los sistemas de TI. El software de automatización funciona dentro de los límites de esas instrucciones, herramientas y marcos para realizar las tareas con muy poca intervención humana (Soaint, s.f.).

2.2.1. ¿Para qué sirve la automatización?

Con la automatización se puede evitar que los procesos repetitivos y manuales los realice el personal de la empresa, permitiendo que los equipos sean más productivos, reduzcan errores, mejoren la colaboración y liberen tiempo que puede ser invertido en tareas más importantes y elaboradas (Red Hat, s.f.b.).

Todo proceso está conformado por tareas y/o actividades y estas pueden simplificarse automatizando dichas actividades; lo cual reducirá el tiempo de ejecución del proceso y reducirá los errores que se puedan presentar al trabajar de forma manual, facilitando las actividades de control.

2.2.2. Beneficios de la automatización

Automatizar los procesos de una empresa permite reducir costos ya que haciendo más eficiente la operación, se logra un mejor uso de los recursos, como, por ejemplo, los sistemas de respaldos. Además, se disminuye significativamente errores humanos que pueden ocurrir de forma manual ocasionando pérdidas. Se logra ahorro de tiempo, debido a que con este sistema de automatización se reducen los intervalos entre una actividad y otra permitiendo así una reducción significativa del tiempo de ejecución para llevar a cabo un determinado proceso (Canales, 2019).

2.2.3. Ventajas de la automatización

La automatización puede ayudar a prevenir el desgaste profesional de los empleados. En la mayoría de los casos, las tareas que se automatizan son aquellas tareas de poco valor.

El aumento de la calidad en los procesos es una ventaja al automatizar, ya que se tendrá el control en los procesos por tener cero errores, por otra parte, la disponibilidad de la ejecución de los procesos ya que seria 24 horas al día.

2.3. Tipos de soluciones RPA

Existen dos tipos de soluciones RPA, estos pueden ser con y sin supervisión, los cuales detallaremos a continuación:

Bots de RPA con supervisión: Se ejecutan de manera local en una estación de trabajo y se encargan de las tareas de interacción con los clientes. Trabajan a la par de las personas, aunque también se pueden activar a partir de eventos del sistema (Red Hat, s.f.c.).

Bots de RPA sin supervisión: Trabajan con los datos de la empresa de manera interna en los servidores backend. Como no hay intervención humana, se activan ante determinados eventos o se programan para ejecutarse a un horario específico (Red Hat, s.f.c.).

Los bots de RPA están preparados para seguir una serie de tareas repetitivas y basadas en reglas y, por lo general, no aprenden sobre la marcha. Si se modifica algún aspecto de la tarea automatizada, el bot típico no logrará darse cuenta por sí solo, por lo que tendrá que volver a entrenarlo o programarlo (Red Hat, s.f.c.).

2.4. Metodología de procesos para Bots

Con el objetivo de medir la carga laboral, y poder determinar la medición de antes y después de RPA en los procesos de una organización, es necesario calcular el tiempo que utiliza para la ejecución de las funciones realizadas para las actividades manuales y la carga operativa que esta genera dentro de una organización.

Para estos procesos se sugiere una metodología cuantitativa con el fin de determinar el margen de error que presentan los procesos manuales, y los costos resultantes, antes y después de la automatización. Es necesario el uso de una metodología para analizar e identificar lógicamente los procesos, para esto es importante tener en cuenta que cada proceso debe de estar bien definido dentro de la organización.

A continuación, se presentarán los 6 pasos fundamentales que debe tener una herramienta RPA y que se deben tener en cuenta al momento de su implementación.

A. Identificación y proyección: en esta primera etapa se deberán determinar los alcances del proyecto, se tendrá claro qué tareas van a ser encomendadas a un robot, cuáles serían los sistemas e interfaces involucrados, se tendría en detalle toda la tarea realizada en el recorrido del proceso, desde el inicio de la tarea hasta su finalización.
B. Diseños para la automatización de proces: en esta segunda etapa se determina la complejidad del proceso, el grueso de los procesos que se van a automatizar de simples a extensos, con el objetivo de tener claridad del alcance. Para este caso es necesario realizar un diseño de un flujo de trabajo, donde se determinen las tareas que se deben de realizar. En esta etapa se debe realizar la elección del software elegido para automatizar.
C. Desarrollo: en esta tercera etapa en donde ya fue elegido el software de automatización, se procede a realizar la implementación del mismo, se deberá asignar un responsable de la gestión del software, estas personas responsables deben de estar al tanto de todas las alertas que presente el software en la ejecución de los procesos, también se deberán tomar todas las medidas de seguridad necesarias para el buen desempeño de la herramienta con el fin de evitar que su implementación incurra en alguna vulnerabilidad.
D. Despliegue de automatización: en esta cuarta etapa se programan las tareas a ejecutar dentro del proyecto, aquí se establece el momento inicial de la puesta en marcha del RPA, y se evalúa el comportamiento del proceso.

E. Trabajo Mancomunado: en esta quinta etapa, todas las dependencias involucradas en el proceso de automatización en conjunto con el software y los participantes trabajarán de una forma unida para evaluar posibles inconsistencias presentadas luego del despliegue de la automatización.
F. Estrategia RPA: esta etapa pertenece a la parte estratégica de la fase aquí basados en los análisis de resultados se planearon nuevas integraciones, siempre con enfoque de mejores resultados asentados en la transformación de los procesos.

Como se observa en la figura 1 están contempladas las fases que constituyen una metodología aplicada a un proceso RPA.

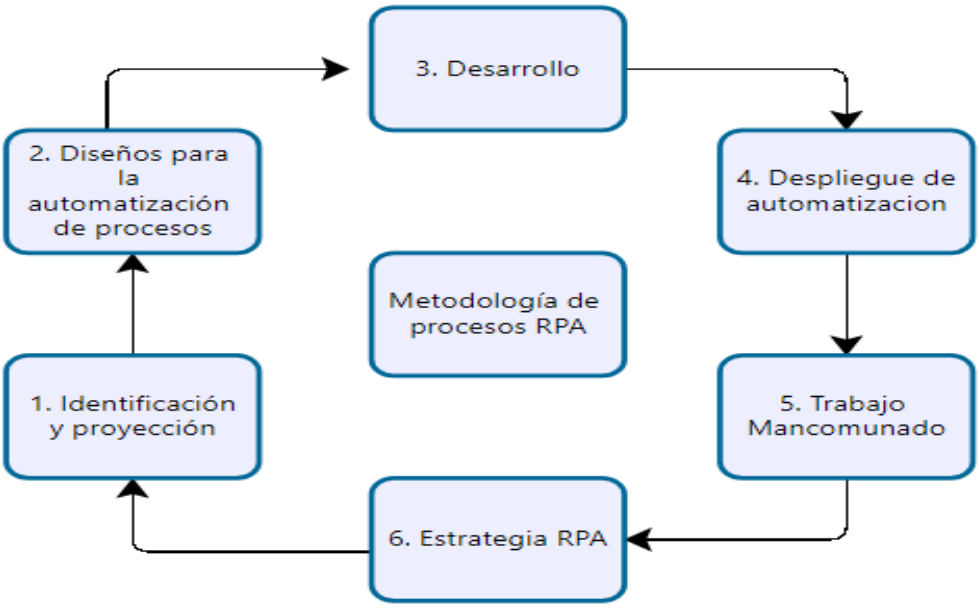

Figura 1. Metodología de procesos. Fuente: elaboración propia.

2.5. Seguridad Informática vs Seguridad de la información

Estos dos conceptos suelen confundirse con facilidad, debido a su similitud gramatical y aunque van de la mano, su significado es diferente. Para la Universidad Cooperativa de Colombia – UCC (2014), la seguridad de la información tiene por objetivo preservar características como la confidencialidad, integridad y disponibilidad de la información. Este concepto tiene asociados temas en un contexto más amplio tales como: la definición de políticas y normas, el control insuficiente de cambios, los riesgos operacionales, el plan de continuidad de negocio, clasificación de la información y matrices de riesgo.

El concepto seguridad informática es fundamentalmente técnico, hace un énfasis en la protección de los sistemas de información, ordenadores, las redes e infraestructura tecnológica (Bermeo-Giraldo et al. 2020). Además, asocia temas en un contexto menor tales como: ataques informáticos, virus, Spam, análisis de vulnerabilidad, Firewall, contraseñas. etc. (UCC, 2014).

De acuerdo con este concepto, es importante mencionar que hay que proteger los datos de las organizaciones, ya que de ellos dependen todos estos pilares que se mencionan anteriormente y que todos los miembros de la empresa debemos considerar que la información, es el activo más importante y que tiene un valor invaluable para su buen funcionamiento. Por lo anterior, y para cumplir con los pilares de la seguridad de la información como los menciona Pérez (2017), se tiene un importante significado como:

- Confidencialidad: A través de ella la seguridad de la información garantiza que los datos que están guardados en el sistema no se divulguen a otras entidades o individuos que no están autorizados para acceder a esa información.
- Disponibilidad: Toda la información que se encuentre recogida en el sistema tiene que estar siempre a disposición de los usuarios autorizados en cualquier momento que ellos necesiten acceder a ella.
- Integridad: Para que el sistema sea veraz los datos no deben manipularse. Así se garantiza que la información recogida sea exacta y no haya sido modificada a no ser que algún usuario autorizado lo haya hecho por orden expresa.

2.5.1. Normas y estándares basados en las buenas prácticas de seguridad de la información.

La seguridad de la información es un requisito para todas las organizaciones y cada día se vuelve más importante dentro de los controles de seguridad y gestión de los riesgos, por esta razón mencionamos el manejo de la norma ISO/IEC 27001 (Sistemas de Gestión de Seguridad de la Información [SGSI], 2017), la cual se encuentra compuesta por diferentes aplicaciones que, al unirlas, trabajan para que la información que manejan las organizaciones no pierda ninguna de sus propiedades más importantes, facilitando el cumplimiento de los requisitos legales y los procesos, para llevar a cabo la implementación de las buenas prácticas de seguridad.

La norma se encuentra centrada en garantizar la confidencialidad, la integridad, la disponibilidad y la autenticidad de la información para intentar evitar las incidencias de tipo físico o lógico que pueda comprometer los niveles de competitividad, de rentabilidad, de conformidad legal y de imagen empresarial, siendo necesarios para conseguir los objetivos de la empresa y asegurar la continuidad del negocio.

2.5.2. Buenas prácticas de seguridad de la información

El uso de la tecnología y la optimización de los procesos juegan un papel muy importante en las organizaciones actuales, ya que esto conjugado dentro de buenas prácticas de seguridad de la información, nos ayudan a gobernar de una forma eficaz y eficiente, no solo desde el punto de vista del cumplimiento de las normas establecidas, sino también hacia la mejora continua en la seguridad de la información, y la gestión inteligente de los objetivos, los cuales nos acercan al éxito.

A continuación, se relacionan tres pautas que determinamos en nuestro artículo, como importantes y determinantes para las buenas prácticas de seguridad de la información.

- Gobierno TI para RPA

Con este gobierno, es importante definir un marco de referencia con funcionalidades y responsabilidades que rijan el comportamiento de los robots, el cual consiste en las imitaciones de las acciones humanas, por lo tanto, se deben de conseguir políticas de gobernabilidad ya definidas antes de iniciar la fase de implementación, las organizaciones deben de evitar al máximo el robo o la pérdida de la información, y el acceso no autorizado a cientos de contenidos de información de datos (Gómez, 2020).

- Arquitectura de seguridad

La Arquitectura de Seguridad de la Información define un esquema de acción estratégico en la organización, mediante el cual se establecen las directrices a nivel de seguridad de la información en cada uno de los procesos del negocio y las técnicas mediante las cuales se pueda salvaguardar, proteger, resguardar los datos digitales e impresos (Parada, Calvo & Flórez, 2011).

- Seguridad de la información

Según (Gómez, 2020) este punto trata de la gestión de credenciales y los accesos para los robots, la segregación de responsabilidades de auditoría en la organización a la hora de utilizar RPA. Algunos puntos que deberían seguirse son:

-El uso de las contraseñas inseguras provoca posibles fugas en la seguridad de la información de una organización. Por ello, es importante establecer una asignación coherente de contraseñas, así como la gestión y el acceso de las contraseñas mediante un administrador de credenciales que las cifre.

-La implementación de controles de seguridad estrictos para no desproteger las credenciales cuando estén en tiempo de ejecución de los robots, en este caso aplicando las normas y estándares de ISO/IEC 27001 que nos ayuda a con las políticas de control de accesos.

En la figura 2 se enuncia una estructura para las buenas prácticas de seguridad de la información, que contemplan los resultados adyacentes de su aplicabilidad en el control de la seguridad de la información y el gobierno TI, la calidad de los servicios entre la seguridad de la información y la arquitectura de seguridad de la información y las políticas establecidas entre el gobierno TI y la arquitectura de seguridad de la información.

Todos estos complementos actuando de manera articulada, aportan mejoras a los procesos en las organizaciones y a su vez mejoran los tiempos de respuesta en los procesos del negocio.

Figura 2. Diagrama de buenas prácticas. Fuente: elaboración propia.

Para la tercera fase de nuestro proyecto, se utlizó una metodología de RPA Seguro, que está basada desde otros marcos de referencia, los cuales explicaremos a continuación. Mencionaremos 3 categorías que consideramos importantes, para indicar algunas pautas dentro de las mejores prácticas de seguridad de la información.

- Seguridad de la información: La tomamos de las normas ISO/IEC 27001, ISO/IEC 27002:2013 (ISO, 2013), siguiendo todas las buenas prácticas que nos propone este marco de referencia, aceptado a nivel nacional e internacional.
- Gobernanza de TI: Lo estamos aplicando basado en los procesos presentados en la "Biblioteca de Infraestructura de Tecnologías de Información" llamado por siglas en inglés ITIL v3.
  La Gestión de Servicios es clave para la Gobernabilidad de TI porque se integra a los objetivos del negocio y hacen que los indicadores y controles sean confiables dentro de una organización (Nextech, 2021).
- Arquitectura de Seguridad: Basándonos en el análisis de la norma ISO 20000-1:2011 (Morán et al., 2007), la cual nos permite gestión de servicios de TI y alcanzando un nivel de calidad aceptable para sus clientes.

3. METODOLOGÍA O DESCRIPCIÓN DEL PROCESO

Para desarrollar los contenidos del tema, de una forma ordenada y secuencial, en las cuales se relacionarán cada una de las fases que propone nuestra investigación. Esta investigación se encuentra propuesta en 3 fases fundamentales en las cuales se contemplan:

Fase 1: Identificación de procesos automatizados: En esta fase se identificará la importancia del RPA en los procesos de las organizaciones frente a la necesidad de crear soluciones autónomas.

Fase 2: Soluciones efectivas por medio de bots: En esta segunda fase analizaremos una solución efectiva por medio de bots, con el fin de automatizar las tareas repetitivas con el objetivo de aumentar la eficacia de los procesos en los sistemas de información.

Fase 3: Buenas prácticas para un RPA seguro: En esta tercera fase analizaremos soluciones basadas a nivel de seguridad que permitan a las organizaciones mejorar sus tiempos de respuesta, basados en el conjunto de las buenas prácticas de seguridad de la información.

4. ANÁLISIS DE RESULTADOS O HALLAZGOS

Fase 1. Identificación de procesos automatizados

Para poder definir con mayor seguridad, si un proceso se puede automatizar dentro de una organización, presentamos las siguientes categorías que consideramos importantes a la hora de implementar una automatización:

A. Identificación

En esta categoría, se debe identificar cuáles son los procesos que se realizan de una manera simple y repetitiva. Estos, corresponden a aquellas tareas que siempre se ejecutan de la misma manera y que llevan una secuencia lógica, es decir, se ejecutan siempre los mismos pasos para entregar la solución.

B. Documentación

Luego de realizar una previa identificación, se procede con la documentación de las tareas a realizar, con el fin de identificar las personas involucradas en estas actividades. Además, se debe llevar una adecuada documentación sobre el software a utilizar y su funcionamiento, detallando paso a paso para cada proceso.

C. Diagrama de trabajo

En la tercera categoría, se debe realizar un diagrama para identificar el flujo de trabajo, para que de una forma más visual se pueda evidenciar el recorrido de cada tarea y adicional, lograr identificar el tiempo aproximado en que se tarda en ejecutarse cada proceso.

A continuación, en la figura 3, encontraremos un diagrama de procesos con los que podemos ver el comportamiento de una tarea desde el inicio hasta el fin, con el objetivo de clasificar sus pasos en acciones estructuradas y totalmente repetitivas, y teniendo como resultado, la identificación de una solución idéntica a las demás actividades realizadas en el día a día por humanos, y notando, además, que su proceso no cambia y, por ende, puede delegarse a un agente virtual o robot.

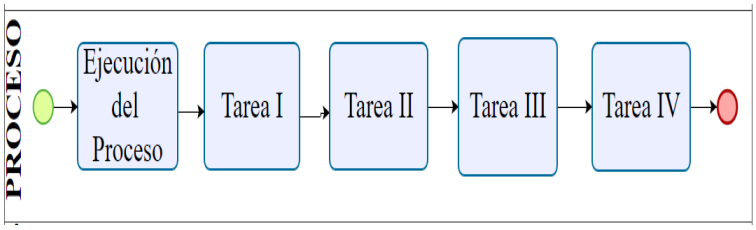

Figura 3. Diagrama de procesos automáticos. Fuente: elaboración propia.

Fase 2. Solución por medio de Bots

En esta segunda fase de nuestro proyecto analizaremos una solución efectiva por medio de bots, con el fin de automatizar las tareas repetitivas y con el objetivo de aumentar la eficacia de los procesos en los sistemas de información

A. Soluciones efectivas por medio de bots

Antes de realizar una creación de un bot, debemos conocer que la mayoría de las herramientas que se utilizan en una organización para la ejecución de actividades en el día a día, son realizadas directamente desde estaciones de trabajo individuales y estas pueden realizar tareas rutinarias, como, mover, filas de datos de una base de datos a una hoja de cálculo. Si bien los bots individuales trabajan en tareas simples, se pueden obtener muchos resultados delegando estas actividades a dichos bots, lo cual puede ser importante para que una empresa funcione de manera más eficiente en los procesos empresariales.

Es posible que la palabra "automatización robótica de procesos" en realidad se trata de los bots de software, la RPA los utiliza para automatizar las tareas repetitivas de las que solían encargarse las personas, ya sean trabajos simples como, por ejemplo, completar formularios y preparar facturas o complejos; para atender a los clientes y resolver problemas, envió de correos de notificación, entre otros.

Un caso práctico es la automatización de las interacciones que mueven los datos entre las aplicaciones que, de no ser por la RPA, estarían aisladas. Un bot puede trabajar dentro de la misma interfaz de usuario que una persona, imitando las acciones como copiar, pegar, extraer datos web, hacer cálculos, abrir y mover archivos, analizar correos electrónicos, iniciar sesión en programas, entre otros.

B. Laboratorio 1. Creación de archivos, por medio de la herramienta Automation Anywhere (s.f.).

A continuación, veremos un pequeño laboratorio, para detallar con más claridad, la manera cómo se puede realizar por medio de un bot; copiar, pegar y abrir un archivo en una ruta específica desde la herramienta Automation Anywhere.

Antes de crear el bot, se debe iniciar sesión en Enterprise Control Room (Automation Anywhere, 2019) a través de la URL de Automation Anywhere Enterprise y agregar un dispositivo local, en este caso conectarlo a mi PC. Por medio de la siguiente figura, se demuestra cómo se conecta un dispositivo, en este caso un pc al software con el que se realizará la práctica.

En la parte superior derecha, se evidencia la conexión al quedar el icono de un pc con una alerta en verde que indica una conexión satisfactoria con la herramienta a utilizar.

Figura 4. Conexión con el software Automation Anywhere. Fuente: elaboración propia.

En esta práctica se creó un bot que va a copiar un archivo de Excel en una ruta nueva, y con el mandato de que cree dicho archivo solo, si este ha sido creado por ejemplo en los últimos 22 días, tarea que se configura para que el bot tenga en cuenta que archivos debo copiar.

En la próxima figura se puede ver la configuración realizada para la tarea del RPA a ejecutar y las rutas seleccionadas en donde se guardarán los archivos creados. Además, la configuración está dada para las fechas en que debe seleccionar los documentos.

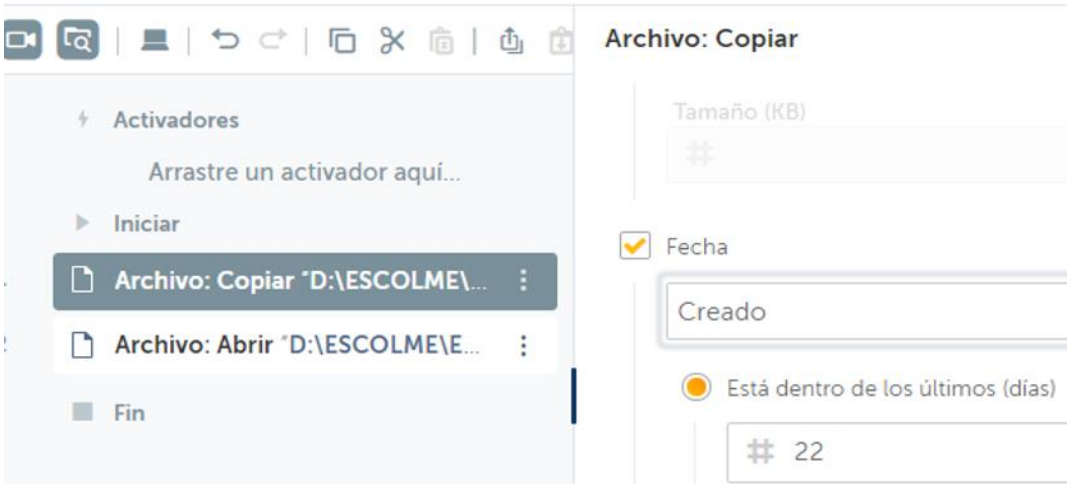

Figura 5. Copiar archivos. Fuente: elaboración propia.

En la figura que se muestra a continuación, se programa una ruta específica para llevar los datos a un nuevo repositorio y que, una vez realizada la copia del archivo, abra dicho archivo para documentarlo y posteriormente guardarlo allí mismo.

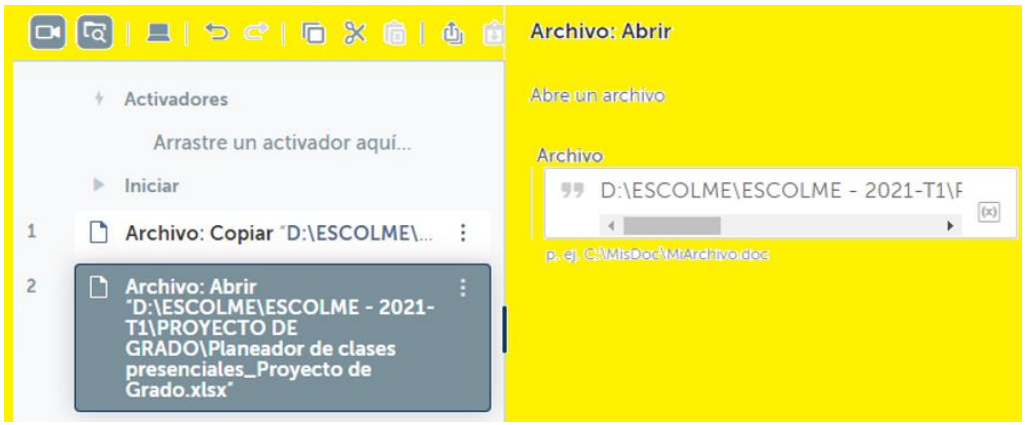

Figura 6. Crear archivos de tipo .xlsx. Fuente: elaboración propia.

Una vez se asigna el mandato al bot, este inicia el proceso de ejecución desde el PC al que se encuentra conectado dicho robot, mostrando, además, el proceso de implementación, el cual puede tardar aproximadamente 30 segundos.

En la siguiente figura, podemos ver que se inicia la descarga de dependencias, las cuales hacen referencia a la configuración anterior, para crear los archivos, además, se puede identificar el tamaño de cada archivo y el porcentaje de ejecución en el que se está llevando a cabo la automatización del proceso.

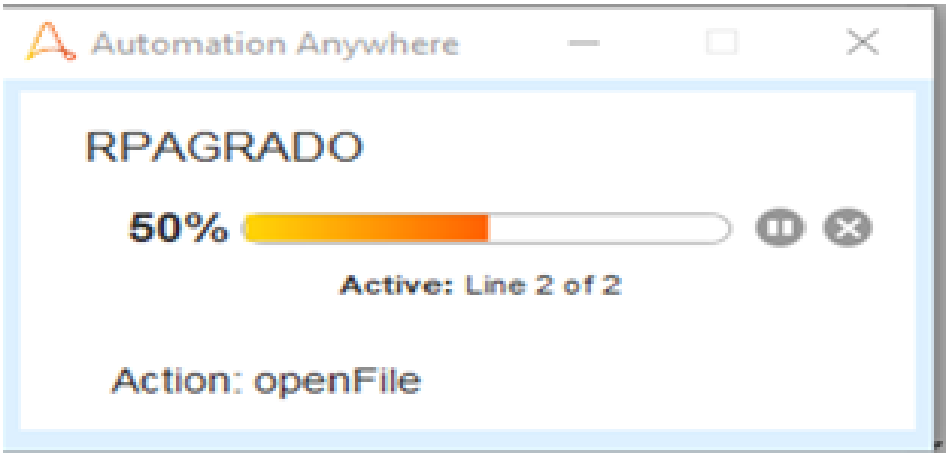

Figura 7. Procesando la información. Fuente: elaboración propia.

Por último, se genera el mensaje de finalización del proceso de implementación RPA, en donde se indica que el bot se ejecutó correctamente.

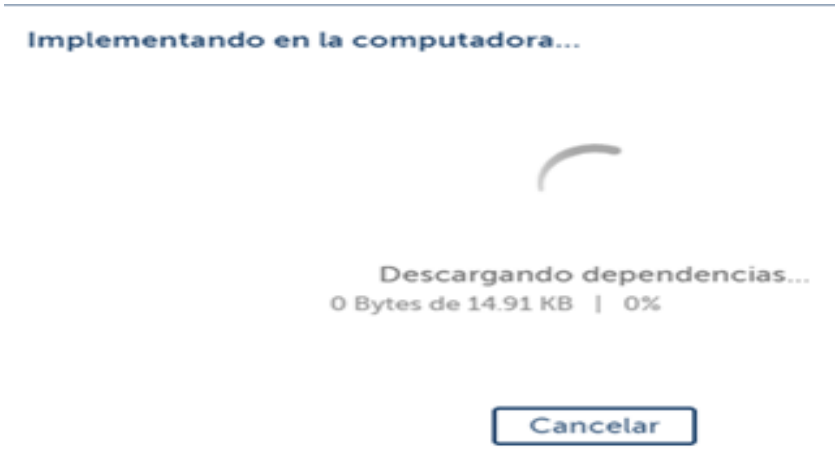

Figura 8. Descarga de dependencias. **Fuente: elaboración propia**.

La figura que veremos a continuación nos muestra un signo de una actividad ejecutada exitosamente, por medio de un robot, y que, además, comprueba que su programación se realizó de manera correcta, dejando como evidencia, la finalización de un proceso exitoso.

Figura 9. Fin del proceso. Fuente: elaboración propia.

Finalmente, se obtiene como resultado, el archivo de Excel listo en la ruta que se programó inicialmente en las tareas a realizar automáticamente por nuestro RPA para los próximos días.

La siguiente figura, nos muestra un documento de tipo .xlsx, creado por un robot, de acuerdo con las tareas encomendadas en los pasos descritos anteriormente.

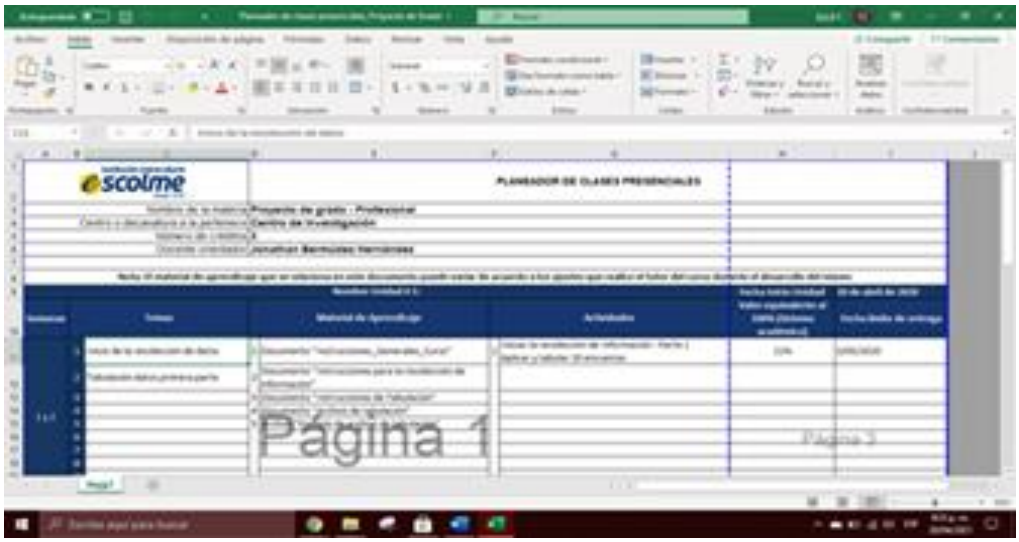

Figura 10. Creación del documento .xlsx. Fuente: elaboración propia.

C. Laboratorio 2. Correos electrónicos por medio de bots con la herramienta UiPath

A continuación, presentamos por medio del software de automatización UiPath (Gimenez, 2020), un robot el cual se programó para realizar envíos de correos a todas las direcciones de correos electrónicos, contenidos dentro de un archivo de Excel.

Esta información puede ser previamente adquirida de una base de datos, en la que el bot estará encargado de ubicar el archivo en una ruta previamente establecida, capturará la información de las celdas y se configurará una variable, en la que se le indique al bot, para que pueda incluir dicha información dentro del correo, y finalmente, procederá a enviar los correos electrónicos.

En la figura 11 que veremos a continuación, se visualizan cuatro etapas de un diagrama de flujo. Estas son las tareas que deben realizarse durante toda la ejecución del robot.

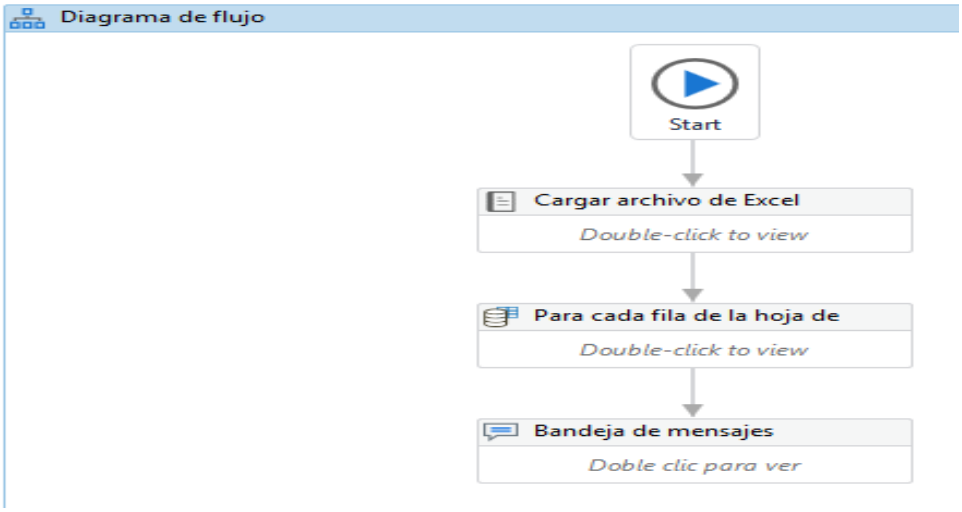

Figura 11. Diagrama de Flujo UiPath. Fuente: elaboración propia.

Etapa uno (Start): Se visualiza un botón donde inician todas las tareas, es decir, el proceso de ejecución del robot.

Etapa dos (Cargar archivo de Excel): se configura el ámbito de Excel, esta es la opción que carga el archivo, aquí nos pide la ruta donde está ubicado dicho documento que contiene toda la información para enviar los correos.

Etapa tres (Para cada fila de la hoja de): se establece la tarea de leer cada celda con el fin de identificar la información que se necesita para diligenciar el correo, en este caso se necesitará saber en qué celda se encuentran las direcciones de correo para poder enviar el correo.

Etapa cuatro (Bandeja de mensajes) en esta última etapa, se crea una notificación, para que cuando se termine el proceso indique si este, se ejecutó correctamente.

En la siguiente figura 12 podemos ver como el proceso se ejecutó correctamente luego de realizadas cada una de las tareas que se encomendaron al robot. Mostrando cómo llega a la bandeja de mensajes exitosamente.

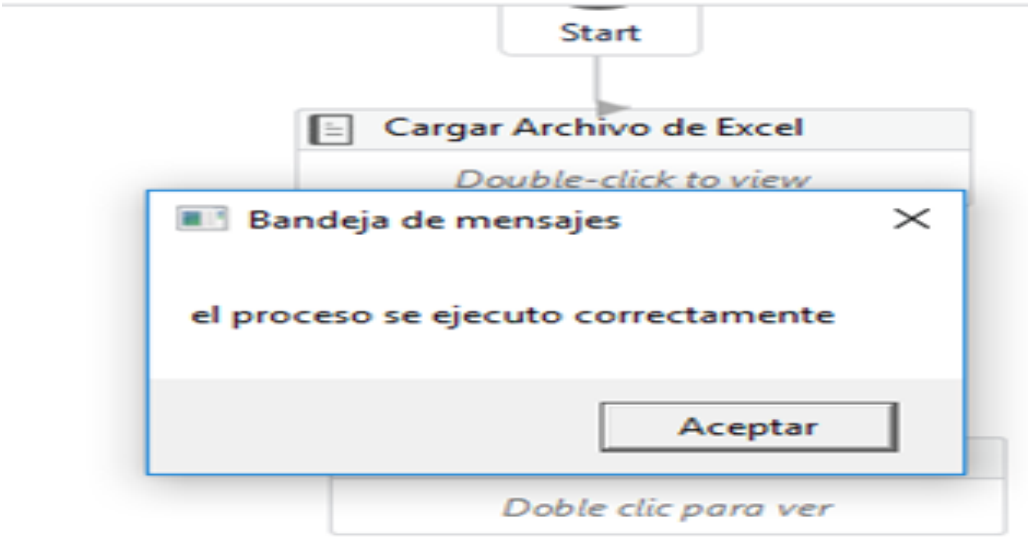

Figura 12. Fin del proceso. Fuente: elaboración propia.

Finalmente se logró automatizar un proceso simple, el cual fue realizar el envío del correo electrónico a cada una de las direcciones contenida en el archivo de Excel, el robot realiza todas las tareas que se configuraron para finalizar el proceso de entrega de dichos correos.

En la figura que observamos a continuación, se detalla una pequeña descripción del mensaje que deja el proceso automatizado de envío de correos electrónicos en la plataforma de correos de Gmail, todo esto fue realizado por medio de un asistente robot o también llamado agente virtual.

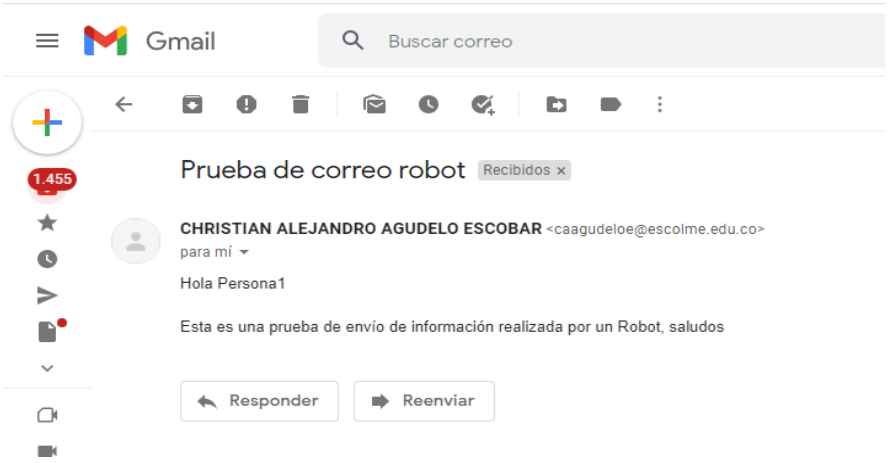

Figura 13. Recepción de correos. Fuente: elaboración propia.

Con las actividades anteriormente presentadas, se logró identificar que el uso de la tecnología RPA mediante los diferentes software o herramientas ya establecidas para la implementación robótica de procesos, nos permite avanzar en los modelos de negocio que se proyecten en las organizaciones. Sin embargo, cabe resaltar la gran diferencia que se puede tener entre el uso de una herramienta con respecto a la otra.

Es decir, el software de Automation Anywhere se puede trabajar de una manera sencilla, y es bastante amigable con el usuario, fácil de instalar, está basada en la web y nativa de la nube para la automatización integral de los procesos y, además, cuenta con la certificación de ISO 27001, lo cual nos genera mucha más confianza al momento de implementar los procesos seguros de la organización.

En cuanto a la herramienta UiPath, podemos decir que su instalación es sencilla e intuitiva, pero su programación un poco compleja, aunque tiene un ambiente gráfico muy agradable, es necesario que se tengan conocimientos amplios en todas sus herramientas y sus funciones, ya que de no conocer todas sus actividades, elementos y tributos se vuelve trabajosa su programación, por eso es necesario tener claro lo que vamos a automatizar, debido a que se debe tener un amplio conocimiento en el proceso de implementación, se pueden presentar complicaciones con el manejo de la herramienta.

Por otra parte, es importante resaltar una parte positiva de este proceso el cual consideramos relevante mencionar, y este es, que, para enviar veinte correos simultáneos, tan solo tomo tres segundos el proceso de recepción, una diferencia realmente considerable, en comparación con un proceso realizado manualmente por una persona en sus labores diarias.

Fase 3. Buenas prácticas para un RPA seguro

En esta tercera fase de nuestro proyecto de investigación queremos proponer una metodología basada en tres pilares fundamentales, los cuales se mencionaron anteriormente en el marco conceptual, con los que se pretende llevar a cabo la implementación de un RPA seguro.

Estos pilares son: seguridad de la información, gobernanza y arquitectura de seguridad.

Para ilustrar con mayor claridad, lo antes indicado, vamos a utilizar el siguiente caso de estudio.

A. Caso de estudio, "Empresa S&C - Mesa de ayuda"

La empresa S&C, tiene como propósito implementar procesos por medio de la automatización robótica de una manera más segura para la organización.

Dentro de los procesos a desarrollar, se tiene como enfoque principal la seguridad, teniendo en cuenta todas las posibles amenazas y vulnerabilidades que se están presentando hoy en día con relación a los datos, evitando riesgos a nivel operativo en la mesa de ayuda.

Aplicación de la propuesta metodológica para RPA seguro:

Para el desarrollo de esta primera parte de nuestra propuesta aplicada sobre el caso de estudio, tomaremos como base para la seguridad de la información, el marco de referencia de la norma ISO/IEC 27001 y los controles en ISO/IEC 27002:2013, aquí brindaremos unas pautas para tener un RPA seguro, y para esto su organización debería responder a las siguientes preguntas:

- ¿Con qué frecuencia analiza los riesgos de seguridad a los que está expuesta su organización?
- ¿Cree usted que automatizar un proceso es realmente seguro y confiable?
- ¿Cuál cree que son las condiciones para un ambiente seguro?
- ¿Cómo está preparada su organización para resolver un ataque de seguridad?
- ¿Su organización posee un software para centralizar las notificaciones o alertas a incidentes de seguridad?

B. Controles caso de estudio

De acuerdo con los controles de seguridad de la información, descritos en la norma ISO/IEC 27002:2013 (ISO, 2013), encontramos los siguientes controles que aplicamos para el caso de estudio, en recomendación como mejores prácticas y soluciones seguras a dicho inconveniente.

Dentro de los 14 Dominios, 35 Objetivos de Control y 114 Controles, estimados en la norma ISO/IEC 27002:2013, tomamos como recomendación los siguientes:

a. Control No 9. Control de Accesos.

Dentro de este control como activo principal de la organización, se busca en función de la seguridad, proteger los datos y la información mediante lista de control de acceso.

Los objetivos del control que se encuentran para la solución a la mesa de ayuda y de acuerdo con la norma son:

- Gestión de acceso de usuario.
- Control de acceso a sistemas y aplicaciones.

Recomendación: Aplicar firewalls basados en host o filtrado de puertos.

- Aplique firewalls basados en host o herramientas de filtrado de puertos en los sistemas finales, con una regla de denegación predeterminada que descarta todo el tráfico, excepto los servicios y puertos que están explícitamente permitidos.

- Una estrategia para la gestión de incidentes con el fin de que no se materialice una amenaza de seguridad es la implementación del firewall, y un cortafuego. Para este caso se sugiere la instalación de un sistema operativo basado en código abierto, relativamente fácil de manejar, donde se logre unificar los eventos de seguridad.

Restricción del acceso a la información.

Procedimientos seguros de inicio de sesión.

La recomendación que se sugiere para este control es:

- Proteja toda la información almacenada en sistemas con listas de control de acceso específicas para sistema de archivos, uso compartido de redes, aplicaciones o bases de datos.

Estos controles harán cumplir el principio de que solo las personas autorizadas deberían tener acceso a la información en función de su necesidad de acceder a la información como parte de sus responsabilidades.

b. Control No 16. Gestión de incidentes en la seguridad de la información.

Dentro de los controles que se encuentran pertinentes para su aplicación son:

- Gestión de incidentes de seguridad de la información y mejoras.
- Responsabilidades y procedimientos.
- Notificación de los eventos de seguridad de la información.
- Notificación de puntos débiles de la seguridad.
- Respuesta a los incidentes de seguridad.
- Aprendizaje de los incidentes de seguridad de la información.

Las recomendaciones que se tienen para este control y aplicándolo a una organización basada en la norma son:

- Documentar los procedimientos de respuesta de incidentes: Asegúrese de que haya planes escritos de respuesta a incidentes que definan las funciones del personal, así como las fases de manejo/gestión de incidentes.

- Asignar cargos y responsabilidades para la respuesta a incidentes: Asigne los cargos y responsabilidades para el manejo, seguimiento y documentación de todos los incidentes cibernéticos a personas específicas hasta que lleguen a una solución.

c. Control No 12. Seguridad en la operativa.

El control que se toma a continuación se considera acorde para el proceso de implementación de la automatización de los procesos.

- Control del software en explotación.
- Instalación del software en sistemas en producción.

La recomendación para el control es:

- Integrar los inventarios de activos de hardware y software: El sistema de inventario de software debe estar vinculado al inventario de activos de hardware para que todos los dispositivos y el software asociado sean rastreados desde una sola ubicación.

Gestión de las vulnerabilidades técnicas

Recomendaciones del control:

Como función de la seguridad, es detectar las vulnerabilidades y de acuerdo con el control se deben ejecutar herramientas de escaneo que permitan detectar las amenazas y vulnerabilidades.

Aplique firewalls basados en host o herramientas de filtrado de puertos en los sistemas finales, con una regla de denegación predeterminada que descarte todo el tráfico, excepto los servidores y puertos que están explícitamente permitidos.

Seguridad en los procesos de desarrollo y soporte, está compuesto por:

- Procedimientos de control de cambios en los sistemas.
- Gestión de cambios.

La recomendación para este control es:

- Utilizar herramientas automatizadas para verificar configuraciones de equipos y detectar cambios: Compare toda la configuración de equipos de red con las configuraciones de seguridad aprobadas definidas para cada dispositivo de red en uso y alerte cuando se descubran desviaciones.

Gobernanza de ITILv3

Para el desarrollo de esta segunda parte de nuestra propuesta, tomaremos como segunda medida el marco de referencia del gobierno de ITILv3, aquí brindaremos unas pautas para aplicar la gobernabilidad para tener un RPA seguro, y para esto su organización debería responder las siguientes preguntas:

- ¿Toma parte el gobierno para definir los objetivos del servicio?
- ¿Cree que la estrategia de los servicios está alineada para que generen valor dentro de la organización?
- ¿Cree que el diseño de los servicios tiene bien definido los objetivos?
- ¿Define usted funciones y responsabilidades dentro de su organización?
- ¿Sabe usted cómo mejorar un proceso dentro de su organización?
- ¿Cuál cree que es el pilar para que un proceso genere valor a su organización?
- ¿Tiene claramente definido cuales son los pasos para definir si una vulnerabilidad afecta sus aplicaciones?

Universalmente la definición adoptada para ITILv3 en cuanto a Gobierno de TI, tiene como consenso general, la importancia de disponer de un marco de referencia para la dirección, administración y control de las infraestructuras y servicios TI, y sus objetivos se limitan exclusivamente a aspectos de gestión.

De acuerdo con las normas del gobierno de ITIL v3, encontramos los siguientes controles que aplicamos para el caso de estudio, en recomendación como mejores prácticas de gobierno en las organizaciones. Se tomaron como referencia los siguientes objetivos propuestos desde ITIL v3.

Fase de Operación del Servicio:

Gestión de Eventos: nueva, como tal, en ITIL v3 es la encargada de monitorizar el rendimiento de la infraestructura TI para la prevención de errores o interrupciones en el servicio.

- Recomendación: monitorizar todos los eventos que acontezcan en la infraestructura TI con el objetivo de asegurar su correcto funcionamiento y ayudar a prever incidencias futuras.

Gestión de Accesos, en conjunto con la Gestión de Seguridad, nos recomienda de acuerdo con la gobernabilidad de ITIL v3 lo siguiente:

- Tomar medidas para prevenir, detectar y evitar ataques contra la organización, procedentes de usuarios.

-Verificación: Comprobar la identidad del usuario que solicita el acceso, así como de aquellos que lo autorizan. También se examina si los motivos para otorgar el acceso son pertinentes.

-Monitorización de identidad. Los cambios en la asignación de permisos suelen estar asociados a un cambio de estatus dentro de la organización: ascensos, despidos, jubilaciones.

Mejora Continua del Servicio: Proporciona una guía para la creación y mantenimiento del valor ofrecido a los clientes a perfiles de un diseño, transición y operación del servicio optimizado.

- Recomendar mejoras para todos los procesos y actividades involucradas en la gestión y prestación de los servicios TI.

- Monitorizar y analizar los parámetros de seguimiento de niveles de servicio y compararlos con los SLAs (Acuerdos de Niveles de Servicios) (Milvus, 2017), establecidos con la organización.

- Dar soporte a la fase de estrategia y diseño para la definición de nuevos servicios y procesos/ actividades asociadas a los mismos.

De acuerdo con las recomendaciones descritas de ITIL v3 para la solución de la mesa de ayuda, encontramos como resultados a esta fase, los siguientes planes de mejoras del servicio:

- Mejorar la calidad de los servicios prestados, incorporar nuevos servicios que se adapten mejor a los requisitos de los clientes y el mercado.

-Mejorar y hacer más eficientes los procesos internos de la organización TI.

Arquitectura de seguridad

Para el desarrollo de esta tercera parte de nuestra propuesta, tomaremos como tercer pilar la arquitectura de seguridad de Parada et al. (2011). La norma ISO/IEC 20000 y la ISO/IEC 20000-1:2011, aquí brindaremos unas pautas para aplica la gestión de los servicios para tener un RPA con un enfoque seguro, para esto su organización debería responder a las siguientes preguntas:

- ¿Cree usted que la arquitectura actual de su organización es la adecuada?
- ¿Cuenta con un sistema de seguridad (firewall) que esté al frente de su organización?
- ¿Conoce qué es una arquitectura de seguridad aplicada a una organización?
- ¿Conoce cuáles son los procedimientos que se deben de implementar para mitigar una vulnerabilidad?
- ¿Cree que actualmente sus políticas de seguridad son suficientes para contrarrestar las vulnerabilidades existentes?

-Una propuesta para el diseño de la arquitectura de seguridad se debe monitorizar y analizar el riesgo de seguridad que se puede tener con las conexiones entre otras aplicaciones como

lo son los servidores de Windows (Active Directory), consultas en bases de datos y todos los entornos donde tenga injerencia el RPA.

De acuerdo con los 13 procesos establecidos en la norma ISO/IEC 20000 (Normas ISO, s.f.) y los procesos de la norma ISO/IEC 20000-1: 2011 (ISO, s.f.) para la gestión de servicios, se mencionarán para nuestro caso de estudio, algunas recomendaciones basadas en la arquitectura de procesos de gestión de servicios de TI y con un enfoque a la mejora continua.

Las recomendaciones establecidas son:

- Una arquitectura de procesos que les permita alinear los procesos de negocio e infraestructura TI y mejorar la calidad de sus servicios con una gestión de servicios de TI ordenada y estructurada.

- Para aplicar la arquitectura de procesos propuesta es necesario que los usuarios principales de cada área de la empresa se comprometan y se identifiquen con los procesos a establecerse, asegurando que el cambio se realice de manera eficiente en sus respectivas áreas.

- La organización mantendrá registro de cada proceso, para tener la confianza necesaria de que los sistemas de seguridad de la información siguen siendo gestionados según lo planificado.

- Definir las categorizaciones de las incidencias y los requerimientos basados en las buenas prácticas de ITIL v3 en conjunto con los estándares de calidad de la norma ISO/IEC 20000-1:2011 (ISO, s.f.). Esto conlleva a determinar las matrices de criticidad basados en los criterios de urgencia e impacto en el servicio.

- Determinar el tipo de software y hardware que presenta mayor necesidad para proyectar de manera eficiente, garantizando un uso idóneo para determinar el tiempo de obsolescencia en los equipos.

- Tener las bases de datos actualizadas, para una posterior renovación tecnológica y mantener la infraestructura en óptimas condiciones de acuerdo con los avances que se vayan presentando tanto a corto como a largo plazo.
Según la estructura de los requerimientos normativos de ISO/IEC 20000-1:2011, tendremos en cuenta los apartados de la norma.

Se definen los requisitos que se deben considerar para asegurar la prestación del servicio. Para nuestro caso estudio “Empresa S&C - Mesa de ayuda” tenemos las siguientes recomendaciones aplicadas en los estándares de la norma:

Operación: Planificación y Control

Operacional: la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos:

▪ Estableciendo los criterios de desempeño para los procesos
▪ Implementando el control de los procesos de acuerdo con los criterios de desempeño

Operación: Aseguramiento del Servicio

Este apartado define los requisitos que se deben considerar para asegurar la prestación de servicios de acuerdo con las necesidades del negocio y los clientes. En este sentido, se requiere:

Gestión de las incidencias de seguridad derivadas del servicio:

▪ Gestión de la Seguridad de la Información utilizada en la prestación de los servicios.

▪ Gestión de las incidencias de seguridad derivadas del servicio: Serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.

▪ Aseguramiento de la Disponibilidad del Servicio y de los recursos que intervienen en el mismo.

▪ Definición y prueba de un Plan de Continuidad, que asegure la continuidad de los servicios y de los recursos involucrados.

Mejora: Aseguramiento de la mejora.

Se establecen los requisitos para que las organizaciones adopten las medidas y procesos necesarios para asegurar que se mejora continuamente la eficacia y la eficiencia de los procesos:

▪ No Conformidades y Acciones Correctivas: Ya no aparecen como tal, las Acciones Preventivas

▪ Mejora continua

5. CONCLUSIONES

Las buenas prácticas que se deben llevar en los procesos de servicio dentro de una organización, como se menciona en el desarrollo de nuestro artículo, estandarizan de forma universal todos los criterios jurídicos y permite evitar las amenazas mediante un enfoque basado en la gestión de riesgos y la normativa de protección de datos, que permiten una posición mucho más ventajosa con respecto a la seguridad de la información para las organizaciones.

Se establecieron pautas para lograr el buen funcionamiento de la tecnología RPA, y un análisis para el conocimiento del negocio de acuerdo con los temas tratados en el transcurso de este artículo, logrando evidenciar que, de ello, depende gran parte las decisiones que se

tomen en una organización para definir cómo llevar a cabo el funcionamiento del modelo de negocio y que, además, estén alineadas con la metodología y las estrategias que se pretendan implementar, permitiendo mejorar sus tiempos de respuestas en conjunto con las buenas prácticas de seguridad de la información.

En un futuro, el procesamiento de los datos se realizará a una escala tan grande, que las organizaciones cambiarán los modelos de servicios y estarán preparadas a encaminarse hacia la excelencia de los procesos con la tecnología RPA, permitiendo que esta, se integre más en los modelos de negocio, ayudando a la estrategia de crecimiento y transformación digital de la organización.

Para adoptar tecnologías como RPA en las organizaciones es importante que los procesos estén bien definidos, se deben dejar atrás las soluciones artesanales, todos los procesos deben de estar siempre bien documentados, con el objetivo de articular la adopción de automatización y poder delegar aquellos procesos que no tienen valor agregado a las organizaciones teniendo como objetivo enfocar la fuerza laboral a aquello que sí representa mayor importancia por su criticidad dentro de la organización.

Se llevaron a cabo pequeños laboratorios o prácticas, con los que logramos demostrar que se pueden crear procesos autónomos que nos permiten crear soluciones efectivas con los bots de RPA, por medio de las diferentes herramientas o software que se implementan en las empresas, logrando reducir sus tiempos de respuesta y mejorando los niveles de servicio en los procesos de las organizaciones.

En las decisiones tomadas por los gerentes de proyectos en las organizaciones, deben considerar la importancia de automatizar los procesos críticos de la organización y saber elegir la mejor herramienta de software para su implementación, de manera que puedan identificar con mayor claridad cuando un procesos o servicio, se puede llegar a trabajar de manera autónoma, a fin de que logren brindar soluciones efectivas en TI.

6. REFERENCIAS

Anagnsote, S. (2018). Robotic Automation Process – The operating system for the digital enterprise. Proceedings Of The International Conference On Business Excellence, 12(1), 54-69. https://doi.org/10.2478/picbe-2018-0007

Automation Anywhere. (s.f). Hacemos que la aceleración digital sea tan fácil como apuntar, hacer clic y listo para la nube. Recuperado de https://www.automationanywhere.com/la/products/automation-360

Automation Anywhere. (2019). Descripción general de Enterprise Control Room. Recuperado de https://docs.automationanywhere.com/es-LA/bundle/enterprise-v11.3/page/enterprise/topics/control-room/getting-started/control-room-overview.html

Bermeo, M. C., Valencia-Arias, A., Garcés, L. F., & García, D. A. (2020). Principales tendencias investigativas en seguridad de redes informáticas a partir del estudio bibliométrico de la literatura desde 1973 al 2019. *En Sepúlveda, J. A (Ed.), Evolución y*

tendencias investigativas en Ingeniería de Sistemas e Ingeniería Industrial (pp. 52-81). Medellín, Colombia: Sello Editorial Coruniamericana.

Canales, R. (2019). ¿Por qué automatizar los procesos de una empresa? Recuperado de https://webpicking.com/por-que-automatizar-los-procesos-de-una-empresa/

Gimenez, M. (2020). Qué es UiPath, todo sobre las funcionalidades de la plataforma RPA. Recuperado de https://www.hiberus.com/crecemos-contigo/que-es-uipath-plataforma-rpa/

Gómez, L. (2020). *Aplicaciones de RPA en el ámbito Empresrial*. (Trabajo de grado, Universidad Politécnica de Madrid). Recuperado de https://oa.upm.es/58123/1/TFG_LAURA_MARIA_GOMEZ_GONZALEZ.pdf

Innovación y Tecnología. (2020). Automatización Robótica de Procesos (RPAs). Recuperado de https://www.innovacion-tecnologia.com/transformacion-digital/automatizacion-robotica-de-procesos-rpa-que-es/

ISO. (2013). ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls. Recuperado de https://www.iso.org/standard/54533.html

ISO. (s.f.). ISO/IEC 20000-1:2011 Information technology — Service management — Part 1: Service management system requirements. Recuperado de https://www.iso.org/standard/51986.html

Mayor-Ríos, J. A., Pacheco-Ortiz, D. M., Patiño-Vanegas, J. C., & Ramos-y-Yovera, S. E. (2019). Análisis de la integración del Big Data en los programas de contaduría pública en universidades acreditadas en Colombia. *Revista CEA*, *5*(9), 53-76. https://doi.org/10.22430/24223182.1256

Milvus. (2017). Configuraciones SLA. Recuperado de https://milvus.online/recursos/sla/

Morán, L., Pérez, A., Trujillo, J., Bathiely, D., & González-Simancas, M. J. (2007). ISO/IEC 20000. Guía completa de aplicación para la gestión de los servicios de tecnologías de la información. España: AENOR.

Mosquera-González, D., Patiño-Toro, O. N., Sánchez-Díez, D. M., Agudelo-Cardona, J. F., OspinaMazo, D. M., & Bermúdez-Bedoya, J. F. (2019). Factores asociados a la calidad en el servicio en Centros de Acondicionamiento Físico a partir del modelo SERVQUAL. *Revista CEA*, *5*(9), 13-32. https://doi.org/10.22430/24223182.1253

Nextech. (2021). ¿Qué es ITIL? – ¿Qué beneficios tiene ITIL? Recuperado de https://nextech.pe/que-es-itil-que-beneficios-tiene-itil/

Normas ISO. (s.f.). ISO 20000 CALIDAD DE LOS SERVICIOS TI. Recuperado de https://www.normas-iso.com/iso-20000/

Parada, D., Calvo, J., & Flórez, A. (2011). Modelo de Arquitectura de Seguridad de la Información – MASI. Recuperado de https://www.iiis.org/CDs2010/CD2010CSC/CISCI_2010/PapersPdf/CA626FI.pdf

Pérez, C. (2017). Seguridad de la información, un conocimiento imprescindible. Recuperado de https://www.obsbusiness.school/blog/seguridad-de-la-informacion-un-conocimiento-imprescindible

Red Hat. (s.f.a.). La automatización completa de la empresa, con herramientas bien definidas y procesoso ptimizados, da paso a la innovación y ofrece claridad a todas sus partes. Recuperado de https://www.redhat.com/es/engage/5-steps-to-automate-your-business-ebook

Red Hat. (s.f.b.). ¿Qué es la automatización? Recuperado de https://www.redhat.com/es/topics/automation/whats-it-automation

Red Hat. (s.f.c.). ¿Qué es la automatización robótica de procesos (RPA)? Recuperado de https://www.redhat.com/es/topics/automation/what-is-robotic-process-automation

Siderska, J. (2021).The Adoption of Robotic Process Automation Technology to Ensure Business Processes during the COVID-19 Pandemic. *Sustainability, 13*(14), 1-20. https://doi.org/10.3390/su13148020

Sistemas de Gestión de Seguridad de la Información -SGSI. (2017). ISO 27001 ¿Cuáles son las buenas prácticas que se utilizan en seguridad de la información? Recuperado de https://www.pmg-ssi.com/2017/10/iso-27001-buenas-practicas-seguridad-informacion/

Soaint. (s.f.). Automatización, sistematiza los procesos de negocio o documentales empleando herramientas tecnológicas. Recuperado de https://soaint.com/automatizacion/

Universidad Cooperativa de Colombia UCC. (2014). Seguridad de la información y seguridad informática, conceptos que debemos conocer y diferenciar. Recuperado de https://www.ucc.edu.co/prensa/2014/Paginas/seguridad-de-la-informacion-y-seguridad-informatica.aspx

Valencia-Arias, A., Bermeo-Giraldo, M. C., Acevedo-Correa, Y., Garcés-Giraldo, L. F., Quiroz-Fabra, J., Benjumea-Arias, M. L., & Patiño-Vanegas, J. (2020). Tendencias investigativas en educación en ciberseguridad: un estudio bibliométrico. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E29), 225-239. Recuperado de https://www.proquest.com/docview/2394537804

Vargas, C. (s.f.). Los beneficios de implementar la Automatización Robótica de Procesos (RPA). Recuperado de https://trycore.co/transformacion-digital/por-que-implementar-la-automatizacion-robotica-de-procesos/

Zelenka, M., & Vokoun, M. (2021). Information and Communication Technology Capabilities and Business Performance: The Case of Differences in the Czech Financial

Sector and Lessons from Robotic Process Automation between 2015 and 2020. *Review of Innovation and Competitiveness: A Journal of Economic and Social Research, 7*(1), 99-116. https://doi.org/10.32728/ric.2021.71/5